Claims, Assertions, Attestations & Certificates (Oh my?)

draft-wiethuechter-drip-identity-claims-03

Adam Wiethuechter

DRIP WG – IETF 109; 18 NOV 2020
A recap

• Draft had a major rewrite to convert to MD
  • Starting to refer to this document as DRIP Proofs
• Discussion on list for what terms to use
  • Started by Stu C. with responses from Carsten B., Michael R., Henk B., Bob M., Michael P.
  • Was clear that we need to put a stake in the ground of what we mean and how it fits in DRIP
• This is my take on what was discussed and how we could proceed and be on the same page
  • Important for Claims, Auth Format, Registry and UAS RID drafts to various degrees
Claim / Assertion

• **Claim**
  • A predicate consisting of two elements
    • **X owns Y**
      • UA owns HHIT and its derivate keypair
    • **X is Y**
      • UA is known by the name "Bob" or something
    • **X belongs to Y**
      • UA belongs to RAA/HDA pairing

• **Assertion**
  • A grouping of one or more claims by an entity
Example Claims / Assertions

• Hierarchical Host Identity Tag (HHIT)
  • HHITs are an **Assertion**
    • Claim 1: Entity owns unique ID (hash) and the keypair
    • Claim 2: Entity is participant of a registry (consists of a RAA and HDA pairing) using hash as unique ID

  • 0011:2233:4455:6677 -- Claim 1
  • D:EADB:EEF -- Claim 2
  • Possible to take prefix (2001:000) and the OGA ID (A) and make them claims
Attestation / Certificate

• Attestation
  • A signed assertion
  • Entity uses a keypair associated with a HHIT to create the structures being defined in draft (in DRIP)
    • Minimum is HHIT/HI pairing
    • Binding relationship between parties (Registry and Operator, Operator and Aircraft, etc.)

• Certificate
  • Identities/Attestations being signed by a third party
  • Do we want this to narrow further by being a "trusted third party" (aka a Registry)?
Example Attestations / Certificates

**Attestations**

- Host Identity
- Expiration Timestamp
- Signature

**Certificates**

- Csk
- Cyy
- Expiration Timestamp
- Signature
The proposed flow with terms

• Registry, Aircraft and Operator creates Attestations on themselves (Arr, Aaa, Aoo)
• Operator creates a Certificate for the relationship between itself and Aircraft (Coa)
• Registry uses Aoo to create a Certificate between itself and Operator (Cro)
• Registry uses at least Coa from Operator to create
  • Certificate between itself, Operator and Aircraft (Croa)
  • Certificate/Attestation of Aircraft being a member of Registry (Cra/Ara)
    • This is used later to create the Offline Attestation/Certificate onboard the Aircraft "live" during flight

DRIP - IETF 109
Offline Attestation / Certificate

- A two-part item
  - Upper portion is generated by Registry using Coa and returned during Aircraft provisioning
    - Will be defined in identity-claims draft?
    - Signature generated using Entity X keypair
  - Lower portion signs upper portion during flight by Aircraft using onboard keypair
    - Will be defined in Auth Formats draft

- Is this a Certificate or Attestation?
  - The Registry portion is very much an Attestation (signed claims/ assertions/ relationship)
  - The whole object however??
    - Bob M. is saying Attestation, lines up with definitions defined

Created by Registry

Created by Aircraft
What needs to change in document...

• Section 1.1 needs to be checked to match what is agreed on
• Certificate: X on X needs to be renamed to Attestation: X on X
  • Make short name be "Self-Attestation"
  • Change "Concise Self-Attestation"
• Attestation: X on Y needs to be renamed to Certificate: X on Y
  • Also make changes to the concise forms (aka short forms)
• Attestation: X on Y (Offline Form) might need a new name or left the same
  • Just give the short name "Offline Attestation" to match Bob M. in UAS RID
• Fix the provision section to realign with above
Other TODOs

• Align the Authentication Formats draft with changes
  • Just minor text changes to properly point to identity-claims draft and include the new structures
  • Add text for the signing over the Offline Attestation structure

• Start helping work on a Registry draft

• Continue AX implementation switch from old style auth to new style auth
  • Halted due to the numerous demos freezing code base
Discussion

Questions, Comments, Concerns?

Title text: For those of you also taking Game Theory, your grade in that class will be based on how close your grade on this exam is to 80% of the average.

https://xkcd.com/1269/